Model Checking Safety and Liveness via k-Induction and Witness Refinement
– Proofs –

Nils Timm and Stefan Gruner

Department of Computer Science, University of Pretoria, Pretoria, South Africa
{ntimm,sgruner}@cs.up.ac.za

In this technical report we present the proofs of Theorem 1, Theorem 2, Lemma 3 and Theorem 3 of the article *Model Checking Safety and Liveness via k-Induction and Witness Refinement*, submitted to the journal *Science of Computer Programming*. In the proofs we make use of Lemma 1, proven in [1], which states that definite (*true* and *false*) temporal logic properties are preserved under three-valued abstraction refinement.

Lemma 1.
Let $Sys = \|_{i=1}^{n} P_i$ over Var be a concurrent system. Let A_a and A_r be sets of atomic predicates over Var with $A_a \subset A_r$. Let $M_a = (S_a, I_a, R_a, L_a, F_a)$ be the three-valued Kripke structure modelling the state space of Sys abstracted over A_a, and let $M_r = (S_r, I_r, R_r, L_r, F_r)$ be the three-valued Kripke structure modelling the state space of Sys abstracted over A_r. Moreover, let ψ be an LTL formula and $k \in \mathbb{N}$ be a bound. Then the following holds:

1. ${}_{A_a}[M_a, I_a \models_{\exists}^{F} \psi]_k = true \;\Rightarrow\; {}_{A_r}[M_r, I_r \models_{\exists}^{F} \psi]_k = true$
2. ${}_{A_a}[M_a, I_a \models_{\exists}^{F} \psi]_k = false \;\Rightarrow\; {}_{A_r}[M_r, I_r \models_{\exists}^{F} \psi]_k = false$

The first theorem that we will prove here is as follows:

Theorem 1.
Let ${}_A[M, I \models_{\exists} \psi]_k$ be a three-valued bounded model checking problem where M is a state space model of a system Sys abstracted over A and ψ is an LTL safety formula defined over A. Then the following holds:

1. $AR({}_A[M, I \models_{\exists} \psi]_k) = true$ *iff* $WRC({}_A[M, I \models_{\exists} \psi]_k) = true$
2. $AR({}_A[M, I \models_{\exists} \psi]_k) = false$ *iff* $WRC({}_A[M, I \models_{\exists} \psi]_k) = false$

Proof of Theorem 1.
The correctness of Theorem 1 follows from the following:

1. If an unconfirmed witness ω can be proven to be spurious in the inner loop of *WRC*, then it is sound to add the corresponding spurious witness constraint $\overline{\sigma}(\omega)$ to the model checking problem in the outer loop. Here soundness means that there exist a level of abstraction characterised by some predicate set A such that for all further refinements characterised by $A' \supseteq A$ model checking with and without the constraint will yield the same result, i.e. the result is not affected by $\overline{\sigma}(\omega)$ (Proposition 1).
2. If using an unconfirmed witness constraint $\sigma(\omega)$ in the inner loop of *WRC* yields a *true* result, then we would also obtain a *true* result without using this constraint (Proposition 2).

Proposition 1. *Let ${}_{A^\omega}[M, I \models_{\exists} \psi]_k$ be a three-valued bounded model checking problem. Moreover, let ω be a spurious witness and $\sigma(\omega)$ be the corresponding constraint. Then the following holds:*

$${}_{A^\omega}[M, I \models_{\exists} \sigma(\omega) \wedge \psi]_k = false \;\Rightarrow\; \exists\, A \text{ with } \forall\, A' \supseteq A : \big({}_{A'}[M, I \models_{\exists} \Sigma_k \wedge \psi]_k \;\equiv\; {}_{A'}[M \models_{\exists} \Sigma_k \wedge \overline{\sigma}(\omega) \wedge \psi]_k \big)$$

Proof of Proposition 1.

$${}_{A^\omega}[M, I \models_{\exists} \sigma(\omega) \wedge \psi]_k = false \qquad \text{(Premise)}$$
$$\equiv\; {}_{A^\omega}[M, I \models_{\forall} \overline{\sigma}(\omega) \vee \neg\psi]_k = true \text{ (Def. 14, Correspondence between ex. and univ. model checking)}$$

We now use the result of this equivalence transformation as a new premise:

$$
\begin{array}{lr}
{}_{A^\omega}[M, I \models_\forall \overline{\sigma}(\omega) \vee \neg\psi]_k = \mathit{true} & \text{(Premise)}\\
\Rightarrow\ \forall A' \supseteq A^\omega : {}_{A'}[M, I \models_\forall \overline{\sigma}(\omega) \vee \neg\psi]_k = \mathit{true} & \text{(Lemma 1)}\\
\Rightarrow\ \forall A' \supseteq A^\omega : {}_{A'}[M, I \models_\exists \Sigma_k \wedge \psi]_k \ \equiv\ {}_{A'}[M, I \models_\exists \Sigma_k \wedge \psi \wedge (\overline{\sigma}(\omega) \vee \neg\psi)]_k & \text{(Conj. of } \psi \text{ with univ. valid property)}\\
\Rightarrow\ \forall A' \supseteq A^\omega : {}_{A'}[M, I \models_\exists \Sigma_k \wedge \psi]_k \ \equiv\ {}_{A'}[M, I \models_\exists \Sigma_k \wedge \overline{\sigma}(\omega) \wedge \psi]_k & \text{(Equivalence transformation)}\\
\Rightarrow\ \exists A \text{ with } \forall A' \supseteq A : \big({}_{A'}[M, I \models_\exists \Sigma_k \wedge \psi]_k \ \equiv\ {}_{A'}[M, I \models_\exists \Sigma_k \wedge \overline{\sigma}(\omega) \wedge \psi]_k\big) & (A := A^\omega)
\end{array}
$$

The result of this implication completes the proof of Proposition 1. □

Proposition 2. *Let* ${}_A[M, I \models_\exists \Sigma_k \wedge \psi]_k$ *and* ${}_{A^\omega}[M, I \models_\exists \psi]_k$ *be three-valued bounded model checking problems with* $A \subseteq A^\omega$*. Moreover, let* ω *be an unconfirmed witness for* ${}_A[M, I \models_\exists \Sigma_k \wedge \psi]_k$ *and let* $\sigma(\omega)$ *be the corresponding constraint. Then the following holds:*

$$
{}_{A^\omega}[M, I \models_\exists \sigma(\omega) \wedge \psi]_k = \mathit{true} \ \Rightarrow\ {}_{A^\omega}[M, I \models_\exists \psi]_k = \mathit{true}
$$

Proof of Proposition 2.

$$
\begin{array}{lr}
{}_{A^\omega}[M, I \models_\exists \sigma(\omega) \wedge \psi]_k = \mathit{true} & \text{(Premise)}\\
\equiv\ {}_{A^\omega}[M, I \models_\exists \sigma(\omega)]_k = \mathit{true} \ \wedge\ {}_{A^\omega}[M, I \models_\exists \psi]_k = \mathit{true} & \text{(Def. 8)}\\
\equiv\ {}_{A^\omega}[M, I \models_\exists \psi]_k = \mathit{true} & \text{(Equivalence transformation)}
\end{array}
$$

The result of this implication completes the proof of Proposition 2. □

The correctness of Theorem 1 follows from Proposition 1 and Proposition 2. □

Next, we prove Theorem 2:

Theorem 2.
Let ϕ_x *be a cause of violation of the three-valued bounded model checking problem* ${}_{A^\omega}[M, I \models_\exists \sigma(\omega) \wedge \psi]_k$ *local to an unconfirmed witness* ω*. Then in bound iteration* $k + j$ *with* $j \in \mathbb{J}$ *it is admissible to extend the cumulative path constraint* Σ_{k+j} *of the corresponding global model checking problem* ${}_A[M, I \models_\exists \Sigma_{k+j} \wedge \psi]_{k+j}$ *as follows:* $\Sigma_{k+j} := \Sigma_{k+j} \wedge \varphi_x$ *where*

$\phi_1 = I_0 \wedge \sigma(\omega)^{sub} \wedge \psi$	$\varphi_1 = \overline{\sigma}(\omega)^{sub}$	$\mathbb{J} = \{0\}$
$\phi_2 = I_0 \wedge \sigma(\omega)^{sub}$	$\varphi_2 = \overline{\sigma}(\omega)^{sub}$	$\mathbb{J} = \mathbb{N}$
$\phi_3 = \sigma(\omega)^{sub} \wedge \psi$	$\varphi_3 = \overline{\sigma}(\omega)^{sub}_j$	$\mathbb{J} = \mathbb{N}$
$\phi_4 = I_0 \wedge \psi$	$\varphi_4 = \mathit{false}$	$\mathbb{J} = \{0\}$
$\phi_5 = \sigma(\omega)^{sub}$	$\varphi_5 = \bigwedge_{l=0}^{j} \overline{\sigma}(\omega)^{sub}_l$	$\mathbb{J} = \mathbb{N}$
$\phi_6 = \psi$	$\varphi_6 = \mathit{false}$	$\mathbb{J} = \{0\}$
$\phi_7 = I_0$	$\varphi_7 = \mathit{false}$	$\mathbb{J} = \mathbb{N}$

Proof of Theorem 2.
We prove Theorem 2 by showing that the following implication holds for each pair ϕ_x and φ_x:

$$
{}_{A^\omega}[M, S \models_\exists \phi_x]_k = \mathit{false}
$$

$$
\Rightarrow
$$

$$
\exists A \text{ with } \forall A' \supseteq A : \forall j \in \mathbb{J} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \equiv {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \varphi_x \wedge \psi]_{k+j}
$$

Case ϕ_1 and φ_1:

$$_{A^\omega}[M, S \models_\exists \phi_1]_k = \mathit{false}$$
(Premise)
$$\equiv \ _{A^\omega}[M, S \models_\exists I_0 \wedge \sigma(\omega)^{sub} \wedge \psi]_k = \mathit{false}$$
(Def. of ϕ_1)
$$\equiv \ _{A^\omega}[M, S \models_\forall \neg I_0 \vee \overline{\sigma}(\omega)^{sub} \vee \neg\psi]_k = \mathit{true}$$
(Def. 14, Correspondence between ex. and univ. model checking)

We now use the result of this equivalence transformation as a new premise:

$$_{A^\omega}[M, S \models_\forall \neg I_0 \vee \overline{\sigma}(\omega)^{sub} \vee \neg\psi]_k = \mathit{true}$$
(Premise)
$$\Rightarrow \ \forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\forall \neg I_0 \vee \overline{\sigma}(\omega)^{sub} \vee \neg\psi]_k = \mathit{true}$$
(Lemma 1)
$$\Rightarrow \ \forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k \ \equiv \ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi \wedge (\neg I_0 \vee \overline{\sigma}(\omega)^{sub} \vee \neg\psi)]_k$$
(Conj. of ψ with univ. valid property)
$$\Rightarrow \ \forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k \ \equiv \ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \overline{\sigma}(\omega)^{sub} \wedge \psi]_k$$
(Equivalence transformation)
$$\Rightarrow \ \exists A \text{ with } \forall A' \supseteq A : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k \ \equiv \ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \overline{\sigma}(\omega)^{sub} \wedge \psi]_k\big)$$
$(A := A^\omega)$
$$\Rightarrow \ \exists A \text{ with } \forall A' \supseteq A : \forall j \in \{0\} : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv \ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \overline{\sigma}(\omega)^{sub} \wedge \psi]_{k+j}\big)$$
(k = k + 0)

Case ϕ_2 and φ_2:

$$_{A^\omega}[M, S \models_\exists \phi_2]_k = \mathit{false}$$
(Premise)
$$\equiv \ _{A^\omega}[M, S \models_\exists I_0 \wedge \sigma(\omega)^{sub}]_k = \mathit{false}$$
(Def. of ϕ_2)
$$\equiv \ \forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\exists I_0 \wedge \sigma(\omega)^{sub}]_{k+j} = \mathit{false}$$
(We have that in M there exists no k-prefix $s_0 \dots s_k$ satisfying $\sigma(\omega)^{sub}$ that starts in an initial state $s_0 \in I$. The validity of this property is not affected when the bound gets increased.)
$$\equiv \ \forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \neg I_0 \vee \overline{\sigma}(\omega)^{sub}]_{k+j} = \mathit{true}$$
(Def. 14, corresp. between ex. and univ. model checking)

We now use the result of this equivalence transformation as a new premise:

$\forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \neg I_0 \vee \overline{\sigma}(\omega)^{sub}]_{k+j} = \mathit{true}$
(Premise)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\forall \neg I_0 \vee \overline{\sigma}(\omega)^{sub}]_{k+j} = \mathit{true}$
(Lemma 1)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi \wedge (\neg I_0 \vee \overline{\sigma}(\omega)^{sub})]_{k+j}$
(Conj. of ψ with univ. valid property)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \overline{\sigma}(\omega)^{sub} \wedge \psi]_{k+j}$
(Equivalence transformation)

$\Rightarrow\ \exists A \text{ with } \forall A' \supseteq A : \forall j \in \mathbb{N} : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \overline{\sigma}(\omega)^{sub} \wedge \psi]_{k+j}\big)$
($A := A^\omega$)

Case ϕ_3 and φ_3:

${}_{A^\omega}[M, S \models_\exists \phi_3]_k = \mathit{false}$
(Premise)

$\equiv\ {}_{A^\omega}[M, S \models_\exists \sigma(\omega)^{sub} \wedge \psi]_k = \mathit{false}$
(Def. of ϕ_3)

$\equiv\ \forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\exists \sigma(\omega)^{sub}_j \wedge \psi]_{k+j} = \mathit{false}$
(We have that in M there exists no k-prefix $s_0 \dots s_k$ satisfying $\sigma(\omega)^{sub}$ that starts in an arbitrary state and ends in a state s_k in which *safe* is violated. Hence, when the bound gets incremented by j, then there exists no $(k+j)$-prefix whose k-suffix satisfies $\sigma(\omega)^{sub}$ and ends in a state s_{k+j} in which *safe* is violated. Hence, there exists no $(k+j)$-prefix satisfying the j-increment $\sigma(\omega)^{sub}_j$ that ends in a state s_{k+j} in which *safe* is violated.)

$\equiv\ \forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \overline{\sigma}(\omega)^{sub}_j \vee \neg\psi]_{k+j} = \mathit{true}$
(Def. 14, corresp. between ex. and univ. model checking)

We now use the result of this equivalence transformation as a new premise:

$\forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \overline{\sigma}(\omega)^{sub}_j \vee \neg\psi]_{k+j} = \mathit{true}$
(Premise)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\forall \overline{\sigma}(\omega)^{sub}_j \vee \neg\psi]_{k+j} = \mathit{true}$
(Lemma 1)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi \wedge (\overline{\sigma}(\omega)^{sub}_j \vee \neg\psi)]_{k+j}$
(Conj. of ψ with univ. valid property)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \overline{\sigma}(\omega)^{sub}_j \wedge \psi]_{k+j}$
(Equivalence transformation)

$\Rightarrow\ \exists A \text{ with } \forall A' \supseteq A : \forall j \in \mathbb{N} : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \overline{\sigma}(\omega)^{sub}_j \wedge \psi]_{k+j}\big)$
($A := A^\omega$)

Case ϕ_4 and φ_4:

$_{A^\omega}[M, S \models_\exists \phi_4]_k = \mathit{false}$
(Premise)
$\equiv$ $_{A^\omega}[M, S \models_\exists I_0 \wedge \psi]_k = \mathit{false}$
(Def. of ϕ_4)
$\equiv$ $_{A^\omega}[M, S \models_\forall \neg I_0 \vee \neg\psi]_k = \mathit{true}$
(Def. 14, Correspondence between ex. and univ. model checking)

We now use the result of this equivalence transformation as a new premise:

$_{A^\omega}[M, S \models_\forall \neg I_0 \vee \neg\psi]_k = \mathit{true}$
(Premise)
$\Rightarrow$ $\forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\forall \neg I_0 \vee \neg\psi]_k = \mathit{true}$
(Lemma 1)
$\Rightarrow$ $\forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k \;\equiv\; {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi \wedge (\neg I_0 \vee \neg\psi)]_k$
(Conj. of ψ with univ. valid property)
$\Rightarrow$ $\forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k \;\equiv\; {}_{A'}[M, S \models_\exists \mathit{false}]_k$
(Equivalence transformation)
$\Rightarrow$ $\exists A$ with $\forall A' \supseteq A : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k \;\equiv\; {}_{A'}[M, S \models_\exists \mathit{false}]_k\big)$
($A := A^\omega$)
$\Rightarrow$ $\exists A$ with $\forall A' \supseteq A : \forall j \in \{0\} : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \;\equiv\; {}_{A'}[M, S \models_\exists \mathit{false}]_{k+j}\big)$
(k = k + 0)

Case ϕ_5 and φ_5:

$_{A^\omega}[M, S \models_\exists \phi_5]_k = \mathit{false}$
(Premise)
$\equiv$ $_{A^\omega}[M, S \models_\exists \sigma(\omega)^{sub}]_k = \mathit{false}$
(Def. of ϕ_5)
$\equiv$ $\forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\exists \bigvee_{l=0}^{j} \sigma(\omega)_l^{sub}]_{k+j} = \mathit{false}$
(We have that in M there exists no k-prefix $s_0 \ldots s_k$ satisfying $\sigma(\omega)^{sub}$ (that starts in an arbitrary state and ends in an state arbitrary state). Hence, when the bound gets incremented by j, then there exists no $(k+j)$-prefix with any infix of length k that satisfies $\sigma(\omega)^{sub}$. Hence, there exists no $(k+j)$-prefix satisfying any l-increment $(\sigma(\omega)^{sub})_l$ with $0 \leq l \leq j$.)
$\equiv$ $\forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \bigwedge_{l=0}^{j} \overline{\sigma}(\omega)_l^{sub}]_{k+j} = \mathit{true}$
(Def. 14, corresp. between ex. and univ. model checking)

We now use the result of this equivalence transformation as a new premise:

$\forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \bigwedge_{l=0}^{j} \overline{\sigma}(\omega)_l^{sub}]_{k+j} = true$
(Premise)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\forall \bigwedge_{l=0}^{j} \overline{\sigma}(\omega)_l^{sub}]_{k+j} = true$
(Lemma 1)

$\Rightarrow\ \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j}\ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi \wedge \bigwedge_{l=0}^{j} \overline{\sigma}(\omega)_l^{sub}]_{k+j}$
(Conj. of ψ with univ. valid property)

$\Rightarrow\ \exists A \text{ with } \forall A' \supseteq A : \forall j \in \mathbb{N} : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j}\ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \bigwedge_{l=0}^{j} \overline{\sigma}(\omega)_l^{sub} \wedge \psi]_{k+j}\big)$
$(A := A^\omega)$

Case ϕ_6 and φ_6:

${}_{A^\omega}[M, S \models_\exists \phi_6]_k = false$
(Premise)

$\equiv\ {}_{A^\omega}[M, S \models_\exists \psi]_k = false$
(Def. of ϕ_6)

$\equiv\ {}_{A^\omega}[M, S \models_\forall \neg\psi]_k = true$
(Def. 14, Correspondence between ex. and univ. model checking)

We now use the result of this equivalence transformation as a new premise:

${}_{A^\omega}[M, S \models_\forall \neg\psi]_k = true$
(Premise)

$\Rightarrow\ \forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\forall \neg\psi]_k = true$
(Lemma 1)

$\Rightarrow\ \forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k\ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi \wedge \neg\psi]_k$
(Conj. of ψ with univ. valid property)

$\Rightarrow\ \forall A' \supseteq A^\omega : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k\ \equiv\ {}_{A'}[M, S \models_\exists false]_k$
(Equivalence transformation)

$\Rightarrow\ \exists A \text{ with } \forall A' \supseteq A : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_k \wedge \psi]_k\ \equiv\ {}_{A'}[M, S \models_\exists false]_k\big)$
$(A := A^\omega)$

$\Rightarrow\ \exists A \text{ with } \forall A' \supseteq A : \forall j \in \{0\} : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j}\ \equiv\ {}_{A'}[M, S \models_\exists false]_{k+j}\big)$
(k = k + 0)

Case ϕ_7 and φ_7:

$$
\begin{aligned}
& {}_{A^\omega}[M, S \models_\exists \phi_7]_k = \mathit{false} \\
& \text{(Premise)} \\
\equiv\ & {}_{A^\omega}[M, S \models_\exists I_0]_k = \mathit{false} \\
& \text{(Def. of } \phi_7\text{)} \\
\equiv\ & \forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\exists I_0]_{k+j} = \mathit{false}
\end{aligned}
$$

(We have that in M there exists no k-prefix $s_0 \dots s_k$ that starts in an initial state $s_0 \in I$. The validity of this property is not affected when the bound gets increased.)

$$
\begin{aligned}
\equiv\ & \forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \neg I_0]_{k+j} = \mathit{true} \\
& \text{(Def. 14, corresp. between ex. and univ. model checking)}
\end{aligned}
$$

We now use the result of this equivalence transformation as a new premise:

$$
\begin{aligned}
& \forall j \in \mathbb{N} : {}_{A^\omega}[M, S \models_\forall \neg I_0]_{k+j} = \mathit{true} \\
& \text{(Premise)} \\
\Rightarrow\ & \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\forall \neg I_0]_{k+j} = \mathit{true} \\
& \text{(Lemma 1)} \\
\Rightarrow\ & \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi \wedge \neg I_0]_{k+j} \\
& \text{(Conj. of } \psi \text{ with univ. valid property)} \\
\Rightarrow\ & \forall A' \supseteq A^\omega : \forall j \in \mathbb{N} : {}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists \mathit{false}]_{k+j} \\
& \text{(Equivalence transformation)} \\
\Rightarrow\ & \exists A \text{ with } \forall A' \supseteq A : \forall j \in \mathbb{N} : \big({}_{A'}[M, S \models_\exists I_0 \wedge \Sigma_{k+j} \wedge \psi]_{k+j} \ \equiv\ {}_{A'}[M, S \models_\exists \mathit{false}]_{k+j} \big) \\
& (A := A^\omega)
\end{aligned}
$$

This completes the proof of Theorem 2. □

Next, we prove Lemma 3:

Lemma 3.
Let $\mathbf{sat_3}\big({}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!]\big) = \mathit{false}$ and let $[\![\sigma(\omega)]\!]_{uc}$ be the constraint-related part of the unsatisfiable core of ${}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!]$. Then there exists a unique sub formula $\sigma(\omega)^{uc}$ of the constraint $\sigma(\omega)$ with $[\![\sigma(\omega)]\!]_{uc} \subseteq [\![\sigma(\omega)^{uc}]\!]$ and $\mathbf{sat_3}\big({}_{A^\omega}[\![M, I, \sigma(\omega)^{uc}, \psi, k]\!]\big) = \mathit{false}$.

Proof of Lemma 3.
For proving Lemma 3, we start with the definition of the propositional logic encoding $[\![\sigma(\omega)]\!]$ of focussing path constraints $\sigma(\omega)$:

Definition 1 (Encoding of Focussing Path Constraints).
Let $A = A_2 \cup A_3$ be a set of atomic predicates where A_2 is the subset of Boolean predicates and A_3 is the subset of three-valued predicates. Then the set of atoms for the propositional logic encoding of focussing path constraints over A and with bound $k \in \mathbb{N}$ is

$$\mathit{Atoms} = \{P_i \mid p \in A_2, 0 \le i \le k\} \cup \{Q_i^t, Q_i^u \mid q \in A_3, 0 \le i \le k\} \cup \{\bot\}.$$

The propositional logic encoding of a focussing path constraint over A and with bound $k \in \mathbb{N}$ is inductively defined as follows.

$$
\begin{array}{lcl}
[\![p_i]\!] & \equiv & \{P_i\} \\
[\![\neg p_i]\!] & \equiv & \{\neg P_i\} \\
[\![q_i]\!] & \equiv & \{Q_i^t, Q_i^u\} \cup \{Q_i^t, \bot\} \cup \{\neg Q_i^u, \bot\} \\
[\![\neg q_i]\!] & \equiv & \{\neg Q_i^t, Q_i^u\} \cup \{\neg Q_i^t, \bot\} \cup \{\neg Q_i^u, \bot\} \\
[\![\psi \wedge \psi']\!] & \equiv & [\![\psi]\!] \cup [\![\psi']\!]
\end{array}
$$

This allows us to construct the encoding $[\![\sigma(\omega)]\!]$ of a given focussing path constraint $\sigma(\omega)$. Our premise is that $\mathbf{sat_3}\big({}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!]\big) = \mathit{false}$. Hence, there exists some unsatisfiable core

$$
{}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!]_{uc} \;=\; [\![M, k]\!]_{uc} \cup [\![I]\!]_{uc} \cup [\![\sigma(\omega)]\!]_{uc} \cup [\![\psi, k]\!]_{uc}.
$$

By definition of an unsatisfiable core we have that $[\![\sigma(\omega)]\!]_{uc} \subseteq [\![\sigma(\omega)]\!]$. Note that $\mathbf{sat_3}\big({}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!]\big) = \mathit{false}$ implies that $\mathbf{sat}\big({}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!][\bot \mapsto \mathit{true}]\big) = \mathit{false}$. Consequently, only clauses of the form $\{P_i\}$, $\{\neg P_i\}$, $\{Q_i^t, Q_i^u\}$ and $\{\neg Q_i^t, Q_i^u\}$ can be part of $[\![\sigma(\omega)]\!]_{uc}$, whereas clauses of the form $\{Q_i^t, \bot\}$, $\{\neg Q_i^t, \bot\}$ and $\{\neg Q_i^u, \bot\}$ will be always satisfied under the over-approximating completion $[\bot \mapsto \mathit{true}]$. Thus, clauses containing a $\bot$ cannot be part of an unsatisfiable core. Hence, when we define a decoding of $[\![\sigma(\omega)]\!]_{uc}$ back into temporal logic we can assume that all clauses are of the form $\{P_i\}$, $\{\neg P_i\}$, $\{Q_i^t, Q_i^u\}$ or $\{\neg Q_i^t, Q_i^u\}$.

Definition 2 (Decoding of Unsatisfiable Core Parts of Encoded Focussing Path Constraints). *Let $[\![\sigma(\omega)]\!]_{uc}$ be the constraint-related part of an unsatisfiable core of the encoding ${}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!]$ and let $0 \le i \le k$. Then the decoding of $[\![\sigma(\omega)]\!]_{uc}$ back into temporal logic is inductively defined as follows:*

$$
\begin{array}{lcl}
[\![\{P_i\}]\!]^{-1} & \equiv & p_i \\
[\![\{\neg P_i\}]\!]^{-1} & \equiv & \neg p_i \\
[\![\{Q_i^t, Q_i^u\}]\!]^{-1} & \equiv & q_i \\
[\![\{\neg Q_i^t, Q_i^u\}]\!]^{-1} & \equiv & \neg q_i \\
[\![[\![\psi]\!] \cup [\![\psi']\!]]\!]^{-1} & \equiv & [\![[\![\psi]\!]]\!]^{-1} \wedge [\![[\![\psi']\!]]\!]^{-1}
\end{array}
$$

Now we define the unique path constraint $\sigma(\omega)^{uc}$ as follows:

$$
\sigma(\omega)^{uc} := [\![[\![\sigma(\omega)]\!]_{uc}]\!]^{-1}.
$$

As a consequence of Definition 1 and Definition 2, we have that $[\![\sigma(\omega)]\!]_{uc} \subseteq [\![\sigma(\omega)^{uc}]\!]$. Since our premise is

$$
\mathbf{sat_3}\big([\![M, k]\!]_{uc} \cup [\![I]\!]_{uc} \cup [\![\sigma(\omega)]\!]_{uc} \cup [\![\psi, k]\!]_{uc}\big) = \mathit{false}.
$$

we can conclude that

$$
\mathbf{sat_3}\big([\![M, k]\!]_{uc} \cup [\![I]\!]_{uc} \cup [\![\sigma(\omega)^{sub}]\!] \cup [\![\psi, k]\!]_{uc}\big) = \mathit{false}
$$

as well.
This completes the proof of Lemma 3. □

Next, we prove Theorem 3:

Theorem 3.
Let ϕ_x be an unsatisfiable core of the encoding ${}_{A^\omega}[\![M, I, \sigma(\omega), \psi, k]\!]$ of a three-valued bounded model checking problem local to an unconfirmed witness ω. Then in bound iteration $k+j$ with $j \in \mathbb{J}$ it is admissible to extend the cumulative path constraint Σ_{k+j} of the encoding ${}_{A}[\![M, I, \Sigma_{k+j}, \psi, k+j]\!]$ of the corresponding global model checking problem as follows: $\Sigma_{k+j} := \Sigma_{k+j} \wedge \varphi_x$ where

$\phi_1 = [\![M, k]\!]_{uc} \cup [\![I]\!]_{uc} \cup [\![\sigma(\omega)]\!]_{uc} \cup [\![\psi, k]\!]_{uc}$	$\varphi_1 \;=\; \overline{\sigma}(\omega)^{uc}$	$\mathbb{J} = \{0\}$
$\phi_2 = [\![M, k]\!]_{uc} \cup [\![I]\!]_{uc} \cup [\![\sigma(\omega)]\!]_{uc}$	$\varphi_2 \;=\; \overline{\sigma}(\omega)^{uc}$	$\mathbb{J} = \mathbb{N}$
$\phi_3 = [\![M, k]\!]_{uc} \cup [\![\sigma(\omega)]\!]_{uc} \cup [\![\psi, k]\!]_{uc}$	$\varphi_3 \;=\; \overline{\sigma}(\omega)^{uc}_j$	$\mathbb{J} = \mathbb{N}$
$\phi_4 = [\![M, k]\!]_{uc} \cup [\![I]\!]_{uc} \cup [\![\psi, k]\!]_{uc}$	$\varphi_4 \;=\; \mathit{false}$	$\mathbb{J} = \{0\}$
$\phi_5 = [\![M, k]\!]_{uc} \cup [\![\sigma(\omega)]\!]_{uc}$	$\varphi_5 \;=\; \bigwedge_{l=0}^{j} \overline{\sigma}(\omega)^{uc}_l$	$\mathbb{J} = \mathbb{N}$
$\phi_6 = [\![M, k]\!]_{uc} \cup [\![\psi, k]\!]_{uc}$	$\varphi_6 \;=\; \mathit{false}$	$\mathbb{J} = \{0\}$
$\phi_7 = [\![M, k]\!]_{uc} \cup [\![I]\!]_{uc}$	$\varphi_7 \;=\; \mathit{false}$	$\mathbb{J} = \mathbb{N}$

Proof of Theorem 3.
The correctness of Theorem 3 immediately follows from the correctness of Theorem 2, Lemma 2 (from the article) and Lemma 3.

This completes the proof of Theorem 3. $\square$

References

1. Timm, N., Gruner, S.: Three-valued bounded model checking with cause-guided abstraction refinement. Science of Computer Programming 175, 37 – 62 (2019), http://www.sciencedirect.com/science/article/pii/S0167642319300206